



OBSAH BEZPEČNOSTNÉHO BULLETINU

| Č. | Identifikátor | Dôležitosť | CVSS Skóre |
|-----|--|------------|------------|
| 01. | Parallels Plesk produkt - bezpečnostná zraniteľnosť | Vysoká | 8.8 |
| 02. | Schneider Electric Easergy P5 a P3 produkty - viacero bezpečnostných zraniteľností | Vysoká | 8.8 |
| 03. | Bentley Nevada 3500 produkt - bezpečnostná zraniteľnosť | Vysoká | 8.2 |
| 04. | FATEK Automation FvDesigner - viacero bezpečnostných zraniteľností | Vysoká | 7.8 |
| 05. | GE Proficy CIMPLICITY-IPM produkt - bezpečnostná zraniteľnosť | Vysoká | 7.5 |
| 06. | Mitsubishi Electric EcoWebServerIII produkt - viacero bezpečnostných zraniteľností | Vysoká | 7.5 |



| | | | | | |
|---------------------|--|----------------------------------|--|-----------------------------------|--------------------------------|
| Dôležitosť | <input type="checkbox"/> Nízka | <input type="checkbox"/> Stredná | <input checked="" type="checkbox"/> Vysoká | <input type="checkbox"/> Kritická | CVSS skóre: 8.8 |
| Klasifikácia | <input checked="" type="checkbox"/> Neutajované / TLP(CLEAR) | | <input type="checkbox"/> Vyhradené | <input type="checkbox"/> Dôverné | <input type="checkbox"/> Tajné |
| Kód sektora (dopad) | | | | | |

Identifikátor

Parallels Plesk produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť Parallels vydala bezpečnostnú aktualizáciu na produkt Plesk, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégia a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

21.02.2022

CVE

CVE-2021-45008

Zasiahnuté systémy

Plesk vo verzii staršej ako 18.0.41 Update 1

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Eskalácia privilégií

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

<https://github.com/AS4mir/CVE-2021-45008/blob/main/README.md>
<https://www.plesk.com/>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45008>
<https://exchange.xforce.ibmcloud.com/vulnerabilities/220138>



| | | | | | |
|---------------------|--|----------------------------------|--|-----------------------------------|--------------------------------|
| Dôležitosť | <input type="checkbox"/> Nízka | <input type="checkbox"/> Stredná | <input checked="" type="checkbox"/> Vysoká | <input type="checkbox"/> Kritická | CVSS skóre: 8.8 |
| Klasifikácia | <input checked="" type="checkbox"/> Neutajované / TLP(CLEAR) | | <input type="checkbox"/> Vyhradené | <input type="checkbox"/> Dôverné | <input type="checkbox"/> Tajné |
| Kód sektora (dopad) | | | | | |

Identifikátor

Schneider Electric Easergy P5 a P3 produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Schneider Electric vydala bezpečnostnú aktualizáciu na produkty Easergy P5 a P3, ktorá opravuje viacero bezpečnostných zraniteľností.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje neautentifikovanému útočníkovi, ktorý sa nachádza v rovnakom sieťovom segmente prostredníctvom zasielania špeciálne vytvorených paketov, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

28.02.2022

CVE

CVE-2022-22722, CVE-2022-22723, CVE-2022-22725

Zasiahnuté systémy

Easergy P5 s firmware vo verzii staršej ako v01.401.101

Easergy P3 s firmware vo verzii staršej ako v30.205

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje<https://us-cert.cisa.gov/ics/advisories/icsa-22-055-03>



| | | | | | |
|---------------------|--|----------------------------------|--|-----------------------------------|--------------------------------|
| Dôležitosť | <input type="checkbox"/> Nízka | <input type="checkbox"/> Stredná | <input checked="" type="checkbox"/> Vysoká | <input type="checkbox"/> Kritická | CVSS skóre: 8.2 |
| Klasifikácia | <input checked="" type="checkbox"/> Neutajované / TLP(CLEAR) | | <input type="checkbox"/> Vyhradené | <input type="checkbox"/> Dôverné | <input type="checkbox"/> Tajné |
| Kód sektora (dopad) | | | | | |

Identifikátor

Bently Nevada 3500 produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť Bently Nevada vydala bezpečnostnú aktualizáciu na produkt 3500, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

28.02.2022

CVE

CVE-2021-32997

Zasiahnuté systémy

Bently Nevada 3500 Rack Configuration vo verzii staršej ako 6.6

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

<https://us-cert.cisa.gov/ics/advisories/icsa-21-231-02>



| | | | | | |
|---------------------|--|----------------------------------|--|-----------------------------------|--------------------------------|
| Dôležitosť | <input type="checkbox"/> Nízka | <input type="checkbox"/> Stredná | <input checked="" type="checkbox"/> Vysoká | <input type="checkbox"/> Kritická | CVSS skóre: 7.8 |
| Klasifikácia | <input checked="" type="checkbox"/> Neutajované / TLP(CLEAR) | | <input type="checkbox"/> Vyhradené | <input type="checkbox"/> Dôverné | <input type="checkbox"/> Tajné |
| Kód sektora (dopad) | | | | | |

Identifikátor

FATEK Automation FvDesigner - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu FvDesigner od spoločnosti FATEK Automation.

Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom zasielania špeciálne vytvorenej požiadavky, vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

24.02.2022

CVE

CVE-2022-21209, CVE-2022-23985, CVE-2022-25170

Zasiahnuté systémy

FvDesigner vo verzii staršej ako 1.5.100 (vrátane)

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.

Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Administrátorom odporúčame limitovať prístup k administratívnejmu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

<https://us-cert.cisa.gov/ics/advisories/icsa-22-055-01>



| | | | | | |
|---------------------|--|----------------------------------|--|-----------------------------------|--------------------------------|
| Dôležitosť | <input type="checkbox"/> Nízka | <input type="checkbox"/> Stredná | <input checked="" type="checkbox"/> Vysoká | <input type="checkbox"/> Kritická | CVSS skóre: 7.5 |
| Klasifikácia | <input checked="" type="checkbox"/> Neutajované / TLP(CLEAR) | | <input type="checkbox"/> Vyhradené | <input type="checkbox"/> Dôverné | <input type="checkbox"/> Tajné |
| Kód sektora (dopad) | | | | | |

Identifikátor

GE Proficy CIMPLICITY-IPM produkt - bezpečnostná zraniteľnosť

Popis

Spoločnosť GE vydala bezpečnostnú aktualizáciu na produkt Proficy CIMPLICITY-IPM, ktorá opravuje bezpečnostnú zraniteľnosť. Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi s právomocami používateľa eskalovať svoje privilégia a následne vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.02.2022

CVE

CVE-2022-21798, CVE-2022-23921

Zasiahnuté systémy

Proficy CIMPLICITY-IPM vo verzii staršej ako January 2022 (Upgrade)

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Eskalácia privilégií

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.
Administrátorom odporúčame limitovať prístup k administratívnejmu rozhraniu a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

<https://us-cert.cisa.gov/ics/advisories/icsa-22-053-01>
<https://us-cert.cisa.gov/ics/advisories/icsa-22-053-02>



| | | | | | |
|---------------------|--|----------------------------------|--|-----------------------------------|--------------------------------|
| Dôležitosť | <input type="checkbox"/> Nízka | <input type="checkbox"/> Stredná | <input checked="" type="checkbox"/> Vysoká | <input type="checkbox"/> Kritická | CVSS skóre: 7.5 |
| Klasifikácia | <input checked="" type="checkbox"/> Neutajované / TLP(CLEAR) | | <input type="checkbox"/> Vyhradené | <input type="checkbox"/> Dôverné | <input type="checkbox"/> Tajné |
| Kód sektora (dopad) | | | | | |

Identifikátor

Mitsubishi Electric EcoWebServerIII produkt - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Mitsubishi Electric vydala bezpečnostnú aktualizáciu na produkt Energy Saving Data Collecting Server (EcoWebServerIII), ktorá opravuje viacero bezpečnostných zraniteľností. Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

28.02.2022

CVE

CVE-2016-10735, CVE-2017-18214, CVE-2018-14040, CVE-2018-14042, CVE-2018-20676, CVE-2019-8331, CVE-2020-11022, CVE-2020-11023, CVE-2020-7746

Zasiahnuté systémy

MES3-255C-EN vo verzii staršej ako v3.3.1
MES3-255C-DM-EN vo verzii staršej ako v3.3.1
MES3-255C-CN vo verzii staršej ako v3.3.1
MES3-255C-DM-CN vo verzii staršej ako v3.3.1

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje<https://us-cert.cisa.gov/ics/advisories/icsa-22-055-02>